## ABSTRACT

Information leaked from smart cards and other tamper resistant cryptographic devices can be statistically analyzed to determine keys or other secret data. A data collection and analysis system is configured with an analog-to-digital converter connected to measure the device's consumption of electrical power, or some other property of the target device, that varies during the device's processing. As the target device performs cryptographic operations, data from the A/D converter are recorded for each cryptographic operation. The stored data are then processed using statistical analysis, yielding the entire key, or partial information about the key that can be used to accelerate a brute force search or other attack.